

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)

TUC920010022US1

I hereby certify that this correspondence is being transmitted via the
USPTO EFS-Web System to Examiner Firmin Backer on:

9/13/2006

Signature

/David Victor/

Typed or printed
name David W. Victor

Application Number

09/977,159

Filed

October 11, 2001

First Named Inventor

G.A. Jaquette

Art Unit

3621

Examiner

Firmin Backer

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

I am the

☐

applicant/inventor.

/David Victor/

☐

assignee of record of the entire interest

Signature

See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

David W. Victor

☒

attorney or agent of record

Registration number 39,867

310-556-7983

Telephone number

☐

attorney or agent acting under 37 CFR 1.34

9/13/2006

Registration number if acting under 37 CFR 1.34

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.

Submit multiple forms if more than one signature is required, see below.

☐

*Total of _____ forms are submitted

This collection of information is required by 35 U.S.C. 132. This information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is guaranteed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	G.A. Jaquette	Examiner	3621
Serial No.	09/977,159	Group Art Unit	Fimmin Backer
Filed	October 11, 2001	Docket No.	TUC920010022US1
TITLE	METHOD, SYSTEM, AND PROGRAM FOR SECURELY PROVIDING KEYS TO ENCODE AND DECODE DATA IN A STORAGE CARTRIDGE		

PRE-APPEAL BRIEF REQUEST FOR REVIEW ARGUMENTS

Applicants request a pre-appeal brief review of the Examiner's rejection of claims 1-43 as anticipated (35 U.S.C. §102(e)) by Kuroda (U.S. Patent No. 6,915,434) in a Final Office Action dated May 12, 2006 ("Final Office Action").

Claims 1, 18, and 27 concern enabling access to data in a storage medium within one of a plurality of storage cartridges capable of being mounted into an interface device and require: providing an association of at least one coding key to the plurality of storage cartridges; encrypting the coding key; and decrypting the encrypted coding key to use to decode and code data stored in the storage medium of the at least one of the storage cartridges.

The Examiner cited FIGs. 1, 2, 11, 13, 16, 22, 23, and 25 and the accompanying text of Kuroda as teaching the claim requirements. (Final Office Action, pg. 2)

The cited FIG. 1 shows a key management unit 2 and encryption unit 3 for a storage apparatus. (Kuroda, col. 5, lines 33-50) The encrypting unit 3 encrypts data using an individual key stored in the storage apparatus that is unique to the apparatus. The cited FIG. 2 shows a configuration of the storage apparatus that stores three types of keys, an individual key unique to the apparatus, a group key, and a public key used when data is transmitted to another group. (Kuroda, col. 5, line 50 to col. 6, line 9). The cited FIG. 11 is a configuration of the storage apparatus that has a master key storage unit storing a master key which is a common key shared by all apparatuses. (Kuroda, col. 9, lines 35-43) The cited FIG. 13 discusses the how to generate a group key. The cited FIG. 16 shows communication between groups of the storage apparatuses. (Kuroda, col. 10, line 65 to col. 11, 17). The cited FIG. 22 shows a method for generating a key, including using the group ID to generate a group key. (Kuroda, col. 12, lines 51-67). The cited FIG. 23 shows the generation and distribution of the group key. (Kuroda, col. 13, lines 1-27). The cited FIG. 25 shows how a program is loaded to realize the storage apparatus. (Kuroda, col. 13, line 52 to col. 14, line 10)

Applicants request review because the Examiner has not identified any part of the above cited figures and their accompanying text which discloses that a coding key associated with a

plurality of storage cartridges is encrypted and decrypted to use to decode and code data stored in the storage medium of at least one of the storage cartridges.

Applicants request review because the cited “group key” of Kuroda is not associated with a plurality of storage cartridges or encrypted then decrypted to use to decode and code data as claimed. According to Kuroda, the “group key” is used to encrypt data transmitted and received between storage apparatuses in the same group. (Kuroda, col. 6, lines 25-33) According to Kuroda, the data stored after being encrypted using an individual key is transmitted after being encrypted using a group key for the same group. (Kuroda, col. 7, lines 53-65).

Applicants request review because the Examiner has not cited any part of Kuroda that discloses that the cited “group key” is encrypted and decrypted for use in decoding and coding data on the storage medium. Instead, the “group key” of Kuroda is used to encrypt data being “transmitted and received between electronic data storage apparatuses in the same or different groups.” The individual key is used to encrypt data being stored. (Kuroda, col. 7, lines 53-65). In fact, Kuroda mentions that data received at a storage apparatus encrypted using the group key is first decrypted using the group key and then encrypted using the individual key. (Kuroda, col. 6, lines 53-65; col. 11, lines 45-55)

In the Response to Arguments, the Examiner cited Kuroda’s individual key. (Final Office Action, pg. 8) However, Kuroda states that the “individual key” is unique to a storage apparatus that is used to encrypt data to store. (Kuroda, col. 5, lines 62-65; col. 6, lines 18-25). Applicants request review because although the cited “individual key” encrypts data on one storage apparatus, the Examiner has not cited any part of Kuroda that discloses that the “individual key” used to encrypt and decrypt data being stored is associated with a plurality of storage cartridges. In fact, Kuroda teaches away from this requirement because according to Kuroda, the “individual key” is “unique” to a storage apparatus. Further, the Examiner has not cited any part of Kuroda that discloses that the “individual key” is encrypted and decrypted.

Yet further, Applicants request review because Kuroda describes the “individual key” as associated with one “electronic data storage apparatus” that encrypts and decrypts data. However, the claims require a group key associated with storage cartridges. Thus, the cited “electronic data storage apparatus” of Kuroda does not satisfy the claim requirement of a storage cartridge having the storage medium, because the “electronic data storage apparatus” of Kuroda is the storage drive performing the writing and encryption, not a storage cartridge to be mounted having the storage medium on which the data is written.

Claims 3, 20, and 29 depend from claims 1, 18, and 27, and further require that the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key is enabled to be used to encode data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

The Examiner cited the sections of Kuroda cited with respect to the independent claims as disclosing the additional requirements of claims 3, 20, and 29. (Final Office Action, pg. 3)

Applicants request review on the grounds that the Examiner has not cited any part of Kuroda that discloses that one key associated with a plurality of storage cartridges is used to encode and decode to the storage mediums of a plurality of storage cartridges. The above discussed Kuroda discusses a group key, but that group key is used to encrypt and decrypt data being transmitted between storage apparatuses. (Kuroda, col. 7, lines 53-65) The cited Kuroda discusses an individual key unique to each storage apparatus used to encrypt and decrypt data on the storage apparatus. However, the Examiner has not cited any part of Kuroda that discloses a coding key associated with a plurality of storage cartridges that is used to encrypt and decrypt data written to storage mediums of a plurality of storage cartridges.

Yet further, the Examiner has not cited any part of Kuroda that discusses associating keys with storage cartridges. Instead, Kuroda discusses keys associated with “electronic data storage apparatus” used to perform the read and writing to storage media.

Claims 6, 23, and 32 depend from claims 1, 18, and 27 and further require transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium. The Examiner cited the sections of Kuroda cited with respect to the independent claims as disclosing the additional requirements of claims 6, 23, and 32. (Final Office Action, pgs. 3-4)

Applicants request review because the Examiner has not cited any part of Kuroda that discloses transmitting an encrypted coding key to an interface device into which a plurality of storage cartridges can be mounted, where the interface devices decrypts the coding key to decode and code data in the storage medium. Instead, the above discussed Kuroda discusses how the storage apparatuses use an individual key to encrypt data to the media and use a group key to encrypt data transmitted between apparatuses. The Examiner has not cited any part of Kuroda that discloses the claim requirement of transmitting an encrypted key to an interface device,

which decrypts the key and then uses such key to code and decode data written to a plurality of storage cartridges to which the key is associated.

Claims 7-9 and 33-35 include further requirements on encrypting and decrypting the coding key with multiple different keys. The Examiner cited the sections of Kuroda cited with respect to the independent claims as disclosing the additional requirements of claims 7-9 and 33-35 (Final Office Action, pgs. 3-4). Applicant request review because the Examiner has not cited any part of Kuroda that discloses encrypting and decrypting the key used to code and decode data in the storage mediums of the cartridges.

Independent claims 10, 23, and 36 concern an interface device for accessing data in a removable storage cartridge including a storage medium coupled to the interface device and require: receiving an encrypted coding key from a host system; decrypting the encrypted coding key; using the coding key to encode data to write to the storage medium; and using the coding key to decode data written to the storage medium.

The Examiner cited the same above cited paragraphs of Kuroda as disclosing the requirements of these claims. (Final Office Action, pg. 5) .

The above discussed Kuroda discusses how each storage apparatus has an individual key to encrypt data to the apparatus and uses a group or public key to encrypt data for transfer to another storage apparatus. Applicants request review because the Examiner has not cited any part of Kuroda that discloses that an interface device to which removable cartridges are coupled receives an encrypted coding key from a host system, decrypts the key and then uses the key to code and decode data in a removable storage cartridge. Instead, the above cited Kuroda discusses how "electronic data storage apparatuses" use keys to encrypt data written to the storage or transmitted. The Examiner has not cited any part of Kuroda that discloses decrypting the encrypted coding key to use to encode and decode data written to the storage medium.

Applicants further request review with respect to dependent claims 11-17, 24-26, and 37-43 which provide additional details about how the coding key may be encrypted and decrypted. The cited Kuroda does not disclose the additional requirements of the dependent claims with respect to how a key is encrypted and decrypted because the Examiner has not cited where Kuroda discloses that the storage apparatuses encrypt and decrypt their individual keys.

For instance, claims 15, 26, and 41 require storing the coding key encrypted with the first key within the storage cartridge; receiving an input/output (I/O) request directed to the storage cartridge; and accessing the encrypted coding key from the storage cartridge, wherein the

accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

Applicants request review because the Examiner has not cited any part of Kuroda that discloses that in response to an I/O request, the encrypted coding key is accessed from the storage cartridge and decrypted using a second key, and using the decrypted coding key to execute the I/O request. As discussed, the cited Kuroda discusses how storage apparatuses use individual keys to encrypt data in their apparatuses and group keys to transmit data between apparatuses. However, the Examiner has not cited where Kuroda discloses that this encrypted coding key is accessed from the storage cartridge and decrypted using a second key in order to use the decrypted coding key to execute the I/O request.

Dated: September 13, 2006

By: /David Victor/

David W. Victor
Registration No. 39,867
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977, Fax: 310-556-7984